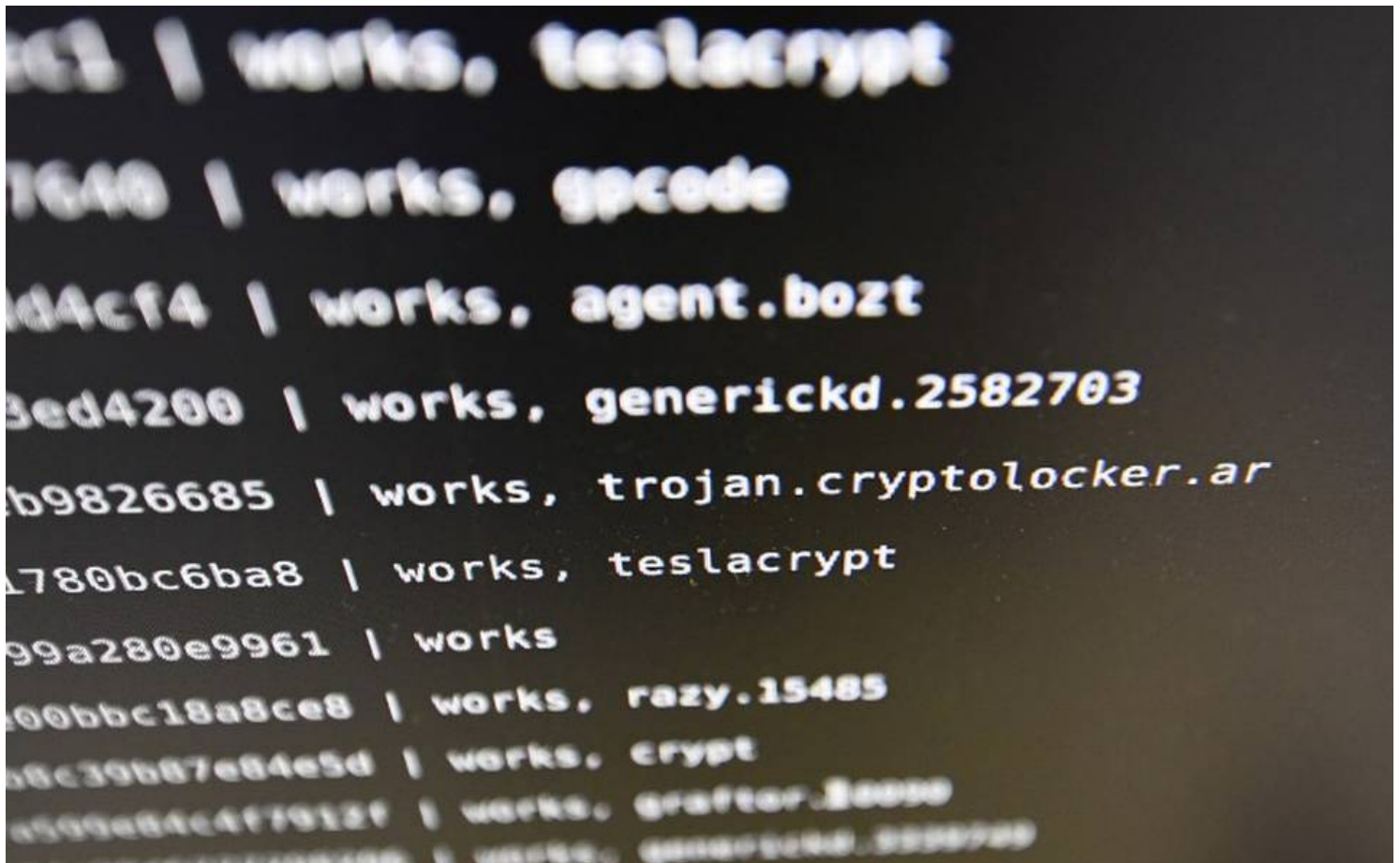


INTERNET

Ransomware attack: India largely safe



Yuthika Bhargava

MAY 13, 2017 21:31 IST

UPDATED: MAY 14, 2017 20:03 IST

For the attack, hackers have used a flaw in Microsoft software to infiltrate unguarded systems.

While no major incident of the worldwide ransomware attack has been reported from India so far, Gulshan Rai, the Cyber Security Chief in the PMO, said a better impact assessment would be possible only on Monday when offices open.

THE HINDU

vulnerability note with a “Severity Rating of High” on March 15 for “a possible remote exploitation of this vulnerability.” The agency advised that the patch released by Microsoft be applied. Over 70 countries have been hit by the cyber attack.

“We have been checking hundreds of systems since we were alerted to this cyber attack. The attacks seem to be the result of a vulnerability in the Microsoft windows OS , and we released a patch,” Mr Rai told *The Hindu*. “We understand systems in Andhra Pradesh are impacted, but so far our assessment is that there isn't much impact,” he added.

CERT-In alert on ransomware attack

Referring to the malware that entered the police cyber networks in Andhra Pradesh, Mr Rai said, “Since this has happened here on the weekend, we are expecting a better impact assessment on Monday.”

ALSO READ

Malware takes
globe hostage

For the attack, which is “perhaps the largest, most widespread and contiguous malware attack in history”, hackers have used a flaw in Microsoft software to infiltrate unguarded systems. “Microsoft had released a patch against this flaw in March but many system administrators failed to patch all computers and the ones which were unpatched became vulnerable to this attack,” Pradipto Chakrabarty, Regional Director, CompTIA India told *The Hindu*.

CompTIA is a global not for profit IT Industry trade body.

CERT-In explained that this ransomware called WannaCrypt or WannaCry encrypts the computer’s hard disk drive and then spreads laterally between computers on the same local area network. The ransomware also spreads through malicious attachments in emails.

Mr Chakrabarty added that the police system in Andhra Pradesh was impacted which may be “because they were using an older version of Microsoft operating system and poor patch maintenance”.

ALSO READ

What is
Ransomware?

Cyber security solution provider Symantec said large number of organizations, particularly in Europe, were impacted. On the other hand Russia-based cyber security firm Kaspersky said it has recorded more than 45,000 attacks of the WannaCry ransomware in 74 countries around

Kaspersky also added that their visibility “may be limited and incomplete and the range of targets and victims is likely much, much higher”.

Tarun Kaura, Director, Product Management – Asia Pacific Japan for Symantec said, “WannaCry has the ability to spread itself within corporate networks, without user interaction, by exploiting a known vulnerability in Microsoft Windows. Computers which do not have the latest Windows security updates applied are at risk of infection.”

Once the ransomware encrypts data files on the affected computer, it asks users to pay the ransom in bitcoins. While the initial payment demanded is of \$300, the ransom note indicates that the payment amount will be doubled after three days. If payment is not made after seven days, the encrypted files will be deleted.

Usually the ransom demand is in the form of crypto currencies such as Bitcoin whose transaction trail is virtually untraceable, Mr Chakrabarty said.

CERT-In, in its advisory issued on Saturday, said that to prevent this infection, users and organisations are advised to apply patches to “Windows systems as mentioned in Microsoft Security Bulletin MS19-010.”

Saket Modi, CEO & Co-Founder of cyber security firm Lucideus said individuals too can be targeted using WannaCry, but since “it’s a ransom worm which means that it automatically hops to another computer in the same network... by targeting an organisation the attack surface for a cyber criminal increases.”

(With inputs from Suhasini Haidar)



Printable version | Mar 8, 2018 11:51:01 AM | <http://www.thehindu.com/sci-tech/technology/internet/cert-in-alert-on-ransomware-attack/article18448177.ece>

© The Hindu